A Hybrid Digital Signature Technique using Cryptosystem

Namrata Vijay
M.Tech
Dept: CSE
TIEIT, Bhopal, M. P

Kaptan Singh
Professor
Dept: CSE
TIEIT, Bhopal, M.P.

Amit Saxena
Head of Department
Dept: CSE
TIEIT, Bhopal, M.P

ABSTRACT
Network is a node collection. The network's basic aim is to transfer information from one location to another. This information must be secured from access by third parties. The cryptography concept was based upon the necessity to secure critical data exchanged across an unsecured network. While using encryption the transmitter encrypts or encodes the information with a secret key so that only the tender recipient will understand it. Cryptanalysis, however, means unwanted access without the secret information key. The cryptography uses various techniques that are Diffie Hellman, AES, RSA, DES, IDEA, BLOWFISH, x.509, PKI, Digital Signatures convert plain texts into the respective chipper text. In different circumstances all these algorithms are important. RSA's most productive computerized signature calculation .This article presents a precise writing review of different computerized signature frameworks dependent on RSA. A basic report is completed on the key age, the creation of marks, the mark check of different computerized signature approaches.

Keywords
Digital Signature, RSA, Cryptography, Key Generation, signature creation, signature verification

1. INTRODUCTION
With the advancement of different system improvement methods, the system security turns out to be increasingly significant. This is considerably progressively significant as clients can get to instruments and alter the data because of the expanding utilization of the World Wide Web. Since the as good as ever, innovation utilized by programmers is presently less secure to share data on the web. The need to confirm basic information traded over an unstable system was the whole idea of cryptography. While utilizing encryption the transmitter will get it. Cryptanalysis, on the other hand, implies undesirable access to data without the mystery key The Greek word for data provided is cryptography. It is in corporate data (Plaintext) change into another structure (Ciphertext). The principle normal for cryptography is confirmation, honesty, and issues regarding security. A convention is the succession of activities structured on minimum couple of sides to meet a goal. In the feeling of the convention, cryptography is additionally related. This convention utilizes 1thecalculation of cryptography and means to quit burglarizing and attack attempts [1]. Governments, organizations, and people these days request safe information in electronic records that are generally mainstream with old reports. Electronic papers require less extra room, practically quick exchanges, and streamlined databases are quite an easy to access. The capacity to utilize data all the more productively has estimated data increment quickly. Regardless, electronic information can defy increasingly more dangerous security risks .Dissimilar to information engraved on paper, information can fundamentally be ransacked from a distant territory in electronic structure. Electronic correspondence changes and blocking is significantly more troublesome than paper-based precursors. The information's security is spoken to by measures to forestall unapproved utilization of electronic information, for example, information disclosure, change, replacement, or pounding. Information insurance is depicted.

1.1 Basic terms used in cryptography [2]
Plaintext-Transparent text is a design that everyone understands readable or original documents. For instance, if A wants to email B+, "Hello," "Hello," here's a clear SMS message.

Cipher text- It's an unreadable message, or after encryption, the resulting message is called a text cipher. For example, "sd45@#$" is a "hello" cipher of text.

Encryption-The simple text method transforms the encryption chip text. The Encryption technique for transmitting sensitive messages via unreliable channels is used in cryptography. An encryption algorithm and a key constitute the basic encryption needs. The method used in encryption is an encryption algorithm. Sender side encryption occurs.

Decoding- A single text called decryption is transformed by the ciphertext method. For decoding the original message from the receiver's ciphertext , cryptography uses the Decryption method. The decryption method has two elements — and key decryption algorithms. The algorithm used in encryption is identical to the algorithm used in decryption.

1.2 Digital Signature Scheme
The digital signature systems may be performed using public-key cryptography. This type of signature recalls an ordinary signature that maybe simple in creation but hard to forge for anyone else. Digital signatures may get permanently linked to signed message content; but it is impossible to move them from document to document because any effort can be made. Digital signatures must also be linked in this Scheme there are two calculations: one to sign, where a mystery key is utilized to develop a message (or an informing hash or both), and one to verify the open key utilized for the legitimacy of the mark. The most used and recognized computerized signature frameworks are RSA and DSA. Computerized marks, (for example, SSL/TLS, numerous VPNs) are integral for the activity of open key frameworks and various system security arrangements.

2. LITERATURE REVIEW
RSA is generally utilized in electronic exchange conventions and its security is dependent on the trouble of enormous numbers deterioration. RSA is protected on the basis of the

reality that it very well may be utilized for open key cryptography, based on the single direction work rule, which can be determined effectively while its converse capacity is troublesome to compute. It utilizes two numerically connected keys, one used in encryption and the other in decryption. Both coding and decoding utilize the key. All things considered; RSA is a calculation dependent on two fundamental numbers. RSA depends on the hypothesis. For securing a wireless network RSA is vital. RSA DSA is a hilter kilter advanced mark calculation that requires a pair of keys one of which must be checked with the other key to sign information. A single direction trap-entryway work depends on RSA DSA. On account of RSA DSA, it is usually simple, yet a lot harder to factor, to increase essential numbers. In polynomial occasions, augmentation is found out in which figuring time can become exponentially as pointed out by the size of the numbers. Dr. Mahmoud T. El-Hadidi et al introduced a product-based execution of a half and half encryption plot for Ethernet LAN. It utilized a key which is in symmetry to the DES-type key for data trade between imparting clients. What's more, a Diffie-Hellmanthe technique is received for key appropriation which consolidates an RSA-type open key plan for making sure about the trading of the symmetric key segments. The disservice was because of the acceptance that by utilizing equipment used for specific pieces of the planned encryption conspires, a lot quicker activity could be acquired.

Cramer and Shoup [4]proposed the main half and half encryption conspire that was handy and is provably secure against versatile picked ciphertext assault under standard unmanageability suspicions.

Louis Granboulan [5] analyzed the two distributed RSA-based cross breed encryption plans having direct reduction with for security evidence: RSA-KEM withDEM1 and RSA-REACT and demonstrated that RSA-KEM+DEM1 ought to be wanted to RSA-REACT. He additionally proposed a few alters to RSA-REACT to improve its effectiveness without changing its security, and the reason this new RSA-REACT is speculation of RSA-KEM+DEM1, with probably similar security, and with potentially more regrettable execution. Kaoru Kurosawa and YvoDesmedt utilized a modification of CramerShoup and got an extremely proficient IND-CCA made sure about half and half encryption plot by utilizing a KEM which isn't IND-CCA secure. This plan was additionally protected in the feeling of IND-CCA under DDH presumption in the regular model. The outcome is additionally summed up to widespread projective hash families.

The ISO/IEC JTC1/SC27normalization council recommends [7] that crossover cryptography can be described as the part of hilter kilter cryptography that utilizes helpful symmetric procedures to expel a section of the issues inalienable in ordinary uneven cryptosystems.

M. Ayoub Khan and Y.P. Singh [8] introduced joint signature and a half and half encryption for security. The recommended plot consolidates the protection of an archive by crossbreed encryption strategy and genuineness by computerized marks. Thought RSA calculation is used for half breed encryption and RSA advanced mark calculation is used to acquire computerized signature (D). The adequacy and precision of the intended plot are outlined through execution and its outcomes. The proposed conspire accomplished a speed of 2.8 Mbps. Y. Wang, and M. Hu under a similar length of key and for a similar extent of the prepared information, RSA is around a few hundred times slower than AES, triple-DES is around multiple times slower than AES, and there are other runtime attributes which further features the distinction between these three cryptographic calculations and gives a reference estimation of two individuals' judicious utilizing. The expanding key length in an instance of RSA and triple-DES when anticipated against key length utilized in Colin D. Walter has proposed a calculation dependent on 'Division Chain' to limit the extent of increases associated with figuring the example. The fundamental preferred position of this plan is that basically no additional memory is required. Besides, the strategy is versatile to a wide range of real assets, giving a variable hunt space from which better assessment request can be established. Noboru Kunihiru and Hirasuke Yamamoto have proposed two strategies viz., a run-length strategy and the half and half technique to create a short expansion chain. C. K. Koc of the National Institute for Standards and Technology introduced a report which as of late proposed Digital Signature Standard (DSS). The accentuation of the report is based on the basic arithmetic , calculations, and their running time examinations. The motive of report is to overcome any barrier between the science of the secluded exponentiation action and its genuine usage on a broadly useful processor. In another report, he proposed RSA equipment usage. IN 1978, R.L. Rivest, A. Shamir, and L. Adlemanproposed a method for executing an open key cryptosystem whose security lays to some extent on the trouble of figuring enormous numbers to allow secure correspondences without the utilization of dispatches to convey keys, and it likewise allows one to "sign" digitized archives. This technique uses elliptic curve cryptography's benefits. In 1984, D. E. Denning [15] distinguished a few properties that ought to be satisfied by any mark; specifically, it ought to obliterate any homographic configuration in the hidden open key calculation. They additionally portrayed marked plot that fulfills these properties. In 2001, Burton S. Kaliski clarified the RSA Digital Signature Scheme and its legitimate issues in detail. Additionally exhorted designers to make an arranged, continuous relocation to an RSA computerized signature conspire offering a few convincing advantages, most prominently provable security, proceeded with utilization of existing RSA keys and equipment quickening agents, and clear, limited programming changes .In 2011, Erfaneh Noorouzi et al presented another advanced mark which works very well for such applications which have low document size for sending. The new hash work produces dynamic and littler sizes of bits that rely upon every byte of the message. A basic instrument for hashing the note and encryption is one of many focal points of interesting calculations. The fundamental capacity which is utilized for hashing is bitwise OR and Multiply works. Testing new calculations demonstrated that its hashed record size is 4% of the first document in messages with a size lower than 1600 bytes. This calculation can be utilized in applications which have low document size for sending and need basic and quick calculations for producing computerized signature. In 2012, PrakashKuppuswamy, Peer Mohammad Appa, and Saeed Q. Y. Al-Khalidi [18] presents another variation of computerized signature calculation which depends on the straight square figure or Hill figure starts with Asymmetric calculation utilizing mod 37 which is quicker and profoundly made sure about. In 2012, Hemant Kumar and Ajit Singh [19] introduced a design is connected with Secure Hash Function and 512-piece SRNN cryptographic calculation. SRNN calculation depends on RSA calculation with some change and included greater security. They additionally planned another calculation for creating the mark that beats the inadequacies of the RSA framework.

Table I. Comparative Table

Reference	Techniques used	Limitations
[3] [12]	DiffieHellman Computation	Computational Overhead
[5 [8][10]	Factorization and Discrete Logarithmic problem	Computational Overhead
[13]	Elgamal Cryptosystem	Computational Overhead
[17]	Hashing	Communication overhead
[18]	Hill Cipher	Computational Overhead
[19]	SRNN	Computational Overhead

3. PROBLEM DEFINITION

To modify the RSA Digital Signature algorithm and evaluate it with another cryptosystem by estimate CPU time for key creation, signature creation, and signature verification.

4. PROPOSED WORK

For providing better security in all aspects we suggested a new scheme i.e. "A New Era of Digital Signature Concepts". The purpose of this dissertation work is:

- To attain Security with a minimum number of overheads. For this work a new algorithm has been built up with some modification in the RSA cryptosystem via a logical concept of the RSA digital signature algorithm cryptosystem as compared to the previous techniques, which provide security at a high level.

- It is clear that key and modulus length plays a significant role in key generation, signature generation, and signature verification process, which is a virtual nucleus of cryptography. If the key/modulus length is slightly changed then almost all the data is also changed so the key management and modulus length is good enough to provide accurate result and enhanced security .Therefore the recommended format is implemented on 2048 bit modulus size.

  This work presents a customized version of RSA Digital Signature algorithm called A New Era of Digital Signature Concepts . By using a well-organized accomplishment of the proposed algorithm, the performance of the algorithm is analyzed by changing various parameters of the algorithm. Our recommended algorithm is based on the two NP-Complete problems named prime factorization and x^{th} root.

4.1 Proposed Algorithm

Proposed public cryptosystem is almost the same as the RSA DSA cryptosystem with some modification. As it is an asymmetrical cryptosystem, it uses two pairs of keys; one key pair is used to encrypt the data in such a way that it can only be decrypted with the other key pair. A common process generates the keys, but they canno tbe generated from each other. Subsequent are the processes of the proposed algorithm.

4.1.1 Key Generation

Followings are the key generation steps:

- Choose two large prime numbersp and q and calculate $n = p \times q$.
- Calculate $\phi(n) = (p-1) \times (q-1)$ and Choose e such that gcd $(e, \phi(n)) = 1$.
- Calculated such that $d \times e \bmod \phi(n) = 1$.
- Choose random numbers b and x. Here x should not relatively prime to $\phi(n)$.
- Calculate c such that $b^x \times c (\text{mod}) n = 1.$
- Public key is (n, e, c, and x) and the private key is (d, b).

4.1.2. Signature Generation

Followings are the signature generation steps:

- Calculate $s_1 = H(m)^d \bmod n.$
- if x|s1 (i.e. x is a divisor of s_1)then generate s_1 again.
- Calculate- $s_2 = (H(m) \times b^{s_1}) \bmod n.$

H (.) is a one-way hash function. (s_1, s_2) is the signature of message m. The sender sends signature with the message m to the receiver.

4.1.3. Signature Verification

Receiver first calculates H (m) using the received message m and check the following two conditions for signature verification:

Verify, if $H(m) = s_1^e \bmod n.$
(1)

and $H(m)^x \equiv s_2^x \times c^{s_1} \bmod n.$
(2)

then the signature is valid else reject the signature.

4.1.4. Proof of Correctness

This section contains the correct proof of the proposed digital signature algorithm. The first condition (equation No. 1) is verification of RSA algorithm and proof of second condition (equation No. 2) isas follows.

R.H.S

$$= (s_2^x \times c^{s_1}) \bmod n$$
$$= (H(m) \times b^{s_1})^x \times c^{s_1} \bmod n$$
$$= H(m)^x \times b^{xs_1} \times c^{s_1} \bmod n$$
$$= H(m)^x \bmod n$$
$$= L.H.S.$$

Now following are the steps of the ERSADSA algorithm-

A. Key Generation Process

- Generate two large random prime no p and q
- Compute n=p*q
- $\phi = (p-1) \times (q-1)$
- Choose an integer e, satisfying $1 < e < \phi$, such that $\gcd(e, \phi) = 1.$
- Compute the secret exponent d $1 < d < \phi$, such that $d \times e \bmod \phi = 1.$
- Choose random numbers b and x.
- Compute c such that $b^x \times c (\bmod) n = 1.$

The public key is (n, e, c, and x) and the private key is (d, b). Keep all the values d, p, q, and ϕ secret .Public key is published for everyone and the private key must be kept secret. Then by using these keys signature generation and signature verification are performed.

B. Signature Generation

Computes $s_1 = H(m)^d \bmod n$

- If x is a divisor of s_1, then generate s_1 again.
- compute $s_2 = (H(m) \times b^{s_1}) \bmod n$
- H ( ) is a one-way hash function. (s_1, s_2) is the signature of message m. the sender sends
- signature with the message m to a receiver.

C. Signature Verification

First compute H(m) using the received message m and check the following two conditions for signature verification verify, if-

$$H(m) = s_1^e \bmod n \text{ =True,}$$

And

$$H(m)^x \equiv s_2^x \times c^{s_1} \bmod n \text{ =True}$$

Then the signature is valid else reject the signature.

D. Proof of Correctness

This section contains the correctness proof of the proposed digital signature algorithm. the First condition (equation No. 1) is a verification of the RSA algorithm and proof of the second condition (equation No. 2) is as follows.

R.H.S

$$= (s_2^x \times c^{s_1}) \bmod n$$
$$= (H(m) \times b^{s_1})^x \times c^{s_1} \bmod n$$
$$= H(m)^x \times b^{xs_1} \times c^{s_1} \bmod n$$
$$= H(m)^x \bmod n$$
$$= L.H.S.$$

5. SIMULATION RESULTS

The work in this dissertation is focused primarily on the improvement of security of public-key cryptosystem, implementation of A New Era of Digital Signature The algorithm, performance analysis of this cryptosystem, and comparison of this cryptosystem with RSA cryptosystem. For the performance analysis, simulation of the algorithm, implemented in JAVA [13], running on a 2.60 GHz P-IV Processor and 1.24 GB RAM. In this section, we investigate the issues of complexity, efficiency, and reliability by running the program with different sets of data. Moreover, a comparison will be done between these different algorithms given the same data as input. The comparison between both algorithms is analyzed by changing only one parameter at a time while keeping the other parameter unchanged. The algorithm depends mainly on the prime number whose value depends on the number of bits used to generate this prime or modulus size. It also depends on the private key; the size of the message digest and the public key [10]. We can show the results through the graph on the basis of the reading in Table 4.1 and 4.2 for the constant public key (512 bit). Table 4.1 and 4.2 show the results for examining key generation, signature generation, and signature verification time for both cryptosystems.

Sensitivity of Changing the Algorithm's Parameters

Both the cryptosystems have some important parameters such as modulus size, private key size, message digest size, and a public key that affect their level of performance. Specifications for the simulation results of both the algorithms are as follows:

1. 2.60 GHz, P-IV Processor with 1.24 GB, RAM.

2. A common message digest 1size of 64 bit is used for key generation, signature generation, and signature verification purposes for both the algorithms.

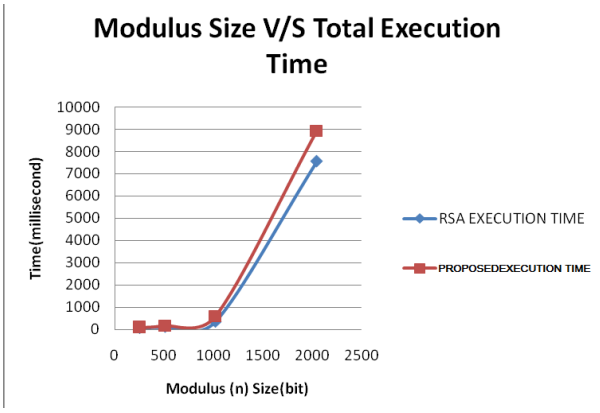
a) Changing the Modulus Length

Changing the modulus affects the other parameters of the algorithms as shown in Table 4.1. It is clear here that increasing the modulus length (bits) increases the bit length of their factors and so the difficulty of factoring them into their prime factors arises. Moreover, the length of the secret key (d) increases at the same rate as the n-bit increases. As a result, increasing the n-bit length provides more security. On the other hand by increasing then-bit length increases the values of key generation time, signature generation time, and signature verification time. Hence increasing the n- bit length increases the security but decreases the rate of key generation, signature generation, and signature verification process as illustrated by Figure 4.1.

Table 5 RSDA Execution

n SIZE	d SIZE	RSADSA Execution Time(ms)				PROPOSED Execution Time(ms)			
		Key Generation Time(ms)(a)	Signature Generation Time(ms)(b)	Signature verification time(ms)(c)	Total Execution time(ms) (a+b+c)	Key Generation Time(ms) (A)	Signature Generation Time(ms) (B)	Signature verification time(ms)(C)	Total Execution time(ms) (A+B+C)
256	256	47	15	15	77	47	16	16	79
512	512	94	16	15	125	110	16	47	173
1024	1024	297	47	16	360	328	94	157	579
2048	2048	7125	344	94	7563	7218	688	731	8637

Fig5. Diagram showing modulus size v/s RSA DSA & PROPOSED Algorithm's execution time, with constant public key size 512 bit and message digest 64 bit.



b) Changing the Public Key Size

Based on simulation results of Table 4.2, following Figure 4.2 shows the effect of public key size on key generation, signature generation, and signature verification time of both the algorithms. Here key generation, signature generation, and signature verification time of both algorithms depend on public key size and as the public key size increases key generation, signature generation, and signature verification time also increases.

e Size	RSADSA Execution Time(ms)				PROPOSED Execution Time(ms)			
	Key Generation Time(ms) (a)	Signature Generation Time(ms) (b)	Signature verification time(ms) (c)	Total Execution time(ms) (a +b +c)	Key Generation Time(ms) (A)	Signature Generation Time(ms) (B)	Signature verification time(ms) (C)	Total Execution time(ms) (A+B+ C)
64	1062	172	15	1249	1062	375	390	1827
128	1953	187	15	2155	1969	375	375	2719
256	1975	187	31	2193	1975	375	391	2741
512	2044	187	47	2278	2059	375	391	2825

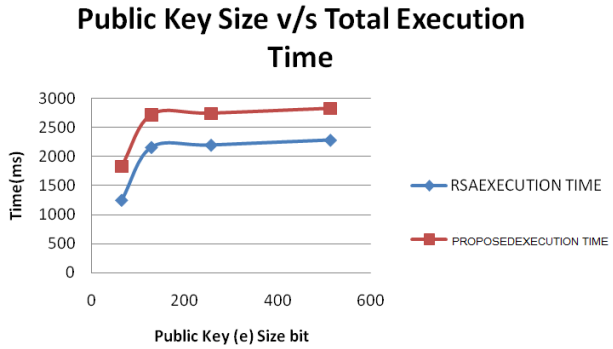


Fig. 5: Diagram showing public key size v/s RSADSA & PROPOSED Algorithm's execution time

5.1 Performance Analysis

Using the criterion presented in [4], the difficulty of each method is estimated as a function of the number of bit operations required. The basic exponential operation here is $a^b \bmod n$ and time complexity of this operation is $O(\log b \times M(n))$, where $M(n)$ the complexity of multiplying two n bit integers. In the suggested algorithm signature generation requires 2modular exponentiation and signature verification requires 4 modular exponentiation which leads to the intricacy of the algorithm to be $O(2 \times \log^3 n)$ and $O(4 \times \log^3 n)$ for signature generation and verification respectively as here $b = O(n)$ and time complexity of multiplying two n bit integers is $O(\log^2 n)$ .Therefore the overall complexity for signature generation and verification is $O(\log^3 n).$ if the complexity of the proposed DSA is compared with other DSA algorithms of the same category (i.e. DSA algorithms that are based on several hard problems) then we see that the Dimitrios Poulakis signature algorithm [25] requires 6modular exponentiation in the signature generation and 2modular exponentiation in signature verification. Ismail E. S signature algorithm [14]requires 5modular exponentiation in the signature generation and 5modular exponentiation in signature verification. Shim in Wei signature algorithm [30] requires 5 modular exponentiation in the signature generation and modular exponentiation in signature verification. So it is clear that the difficulties of such algorithms are equivalent to the majority of the algorithms which are based on prime factorization and discrete logarithm and that is $O(\log^3 n).$

6. CONCLUSIONS

RSA is the asymmetric cryptography system. The security of the RSA public-key cryptosystem is based on the hypothesis that factoring a large number (modulus) is difficult. In RSA if the modulus is factored into its prime numbers then the private key is also detected and hence the security of the cryptosystem is broken. This work presents a modified version of RSA Digital Signature algorithm called A New Era of Digital Signature Algorithm. It is quite impossible in today's aspect to find two prime numbers whose product is the given number. As the size of the number increases, the possibility for factoring the number decreases. In RSA, if one can factor modulus into its prime numbers then he can obtain the private key too. To improve the security, proposed is developed, which is based on the two hard problems called prime factorization and xth root. It is shown that the new algorithm is secure enough against various attacks and one has to solve both the problems for cryptanalysis of the proposed algorithm. The performance analysis is done based on modulus length, private key, public key, key generation time, signature generation time, and signature verification time. A New Era of Digital Signature Algorithm provides far better security against Key-Only attack, Blinding, Known Partial Key attack in comparison of RSA Digital Signature Algorithm. The performance of the suggested algorithm is comparatively equivalent to the majority of the digital signature algorithms which are based on various hard problems. The disadvantage of the new cryptosystem is that, unlike RSA digital Signature Algorithm it cannot be used for authentication as it is based on the one-way function. Another disadvantage is the slowdown of execution process with respect to the RSA Digital Signature Algorithm. But it is clear from the mock results that it provides more security than the RSA Digital Signature Algorithm. However, Chosen-message attacks like RSA DSA can break the safety of the above-described algorithm.

7. REFERENCES

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.

[3] Dr. Mahmoud T. El-Hadidi, Dr. N. H. Hegazi and H. K Aslan, "Implementation of a Hybrid Encryption Scheme

for Ethernet," in Proceedings of Computers and Communications IEEE Symposium, 1995, pp. 150-156.

[4] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in Advances in Cryptology - {CRYPTO} '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, 23-27 August 1998, pp. 13-25.

[5] Louis Granboulan, "RSA hybrid encryption schemes," IACR Cryptology ePrint Archive, p. 110, 2001, [Online].

[6] Kaoru Kurosawa and YvoDesmedt, "A New Paradigm of Hybrid Encryption Scheme," in Advances in Cryptology - {CRYPTO} 2004, Proceedings of 24th Annual International Cryptology Conference, Santa Barbara, California, USA, 15-19 August, 2004, pp. 426-442.

[7] "ISO/IEC 18033-1, Information technology - Security techniques - Encryption Algorithms - Part1 : General," International Organization for Standardization, 2003.

[8] M. Ayoub Khan and Y.P.Singh, "On the security of Joint Signature and Hybrid Encryption," in Networks ,13th IEEE International Conference (Volume:1), 2005.

[9] Y. Wang and M. Hu, "Timing evaluation of the known cryptographic algorithms," in International Conference on Computational Intelligence and Security, 2009, pp. 233-237.

[10] Colin D. Walter, "Exponentiation Using Division Chains," IEEE transactions on Computers, vol. 47, no. 7, 1998.

[11] Noboru Kunihiro and Hirosuke Yamamoto, "New Methods for Generation of Short Addition Chains," IEICE Trans. Fundamental, vol. 83, no. 1, 2000.

[12] C. K. Koc, "High-speed RSA implementations," Technical notes TR 201, RSA Security Inc., Nov. 1994.

[13] C. K. Koc, "RSA hardware implementation," Technical Notes TR 801, RSA Security Inc., Aug. 1995.

[14] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[15] Dorothy E. Denning , "Digital signature with RSA and other Publickey cryptosystems," Comm. of the ACM, vol. 27, no. 4, pp. 388-392, Apr. 1984.

[16] Burton S. Kaliski, "RSA Digital Signatures," Dr. Dobb's Journal, May 2001, [Online]. http://www.drdobbs.com/rsa-digitalsignatures/184404605.

[17] Erfaneh Noorouzi1, Amir Reza EstakhrianHaghighi, FarzadPeyravi and Ahmad, "A new digital signature algorithm," in International Conference on Machine Learning and Computing, vol. 3, Singapore, 2011, pp. 141-146.

[18] Prakash Kuppuswamy, Peer Mohammad Appa and Saeed Q Y AlKhalidi, "A New Efficient Digital Signature Scheme Algorithm based on Block cipher," IOSR Journal of Computer Engineering, vol. 7, no. 1, pp. 47-52, Nov. 2012.

[19] Hemant Kumar, Ajit Singh, "An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography," International Journal of Research Review in Engineering Science and Technology, vol. 1, no. 1, pp. 54-57, Jun. 2012.